Verfahrensverzeichnis
für GdW-Unternehmen

(z. B.) Wohnungsvergabe

Erstellt am XX.XX.2018

nur für den internen Gebrauch

- vertraulich -

Inhaltsverzeichnis

1. GdW-Unternehmen

Allgemeines

Das Verfahrensverzeichnis enthält alle gesetzlich geforderten Informationen über die bei der "Name des GdW-Unternehmens" und den angeschlossenen Unternehmen durchgeführten Verarbeitungen von personenbezogenen Daten, deren nähere Angaben, den Stand der Prüfungen, etc.

Name:	GdW-Unternehmen
Telefon:	xxx / xxx xxxxxxx
Telefax:	xxx / xxx xxxxxxx
E-Mail:	info@musterwohn.de
Postanschrift:	Musterstraße xxxxx Musterstadt Deutschland

"GdW-Unternehmen" wird vertreten durch:

Geschäftsführer/Vorstand:
NAME/VORNAME

Zuständige Aufsichtsbehörde:

Name:	z. B. Bayerisches Landesamt für Datenschutzaufsicht		
Telefon:	+49 981/53-1300		
Telefax:	+49 981/53-5300		
E-Mail:	poststelle@lda.bayern.de		
Postanschrift:	Promenade 27 (Schloss) 91522 Ansbach	Besucher-anschrift:	Promenade 27 (Schloss) 91522 Ansbach

Datenschutzbeauftragte(r)

Zum Datenschutzbeauftragten des Unternehmens "Name des GdW-Unternehmens" ist DSB Vorname DSB Name bestellt.

Name:	DSB Name	Telefon:	xxx / xxx xxxxxxx
Vorname:	DSB Vorname	Mobil:	XXXX / XXX XXXXXXXX
Position:	externer Datenschutzbeauftragter	Telefax:	XXX / XXXXX XXXX
Abteilung:	Consulting (externer Dienstleister)	E-Mail:	XXX.XXXX@XXX.de
Postanschrift:	DSB Straße XXXXX DSB ORT Bayern Deutschland		

Stellvertr. Datenschutzbeauftragte(r)

Name:	stellvertr. DSB Name	Telefon:	xxx / xxx xxxxxxx
Vorname:	stellvertr. DSB Vorname	Mobil:	XXXX / XXX XXXXXXXX
Position:	externer Datenschutzbeauftragter	Telefax:	XXX / XXXXX XXXX
Abteilung:	Consulting (externer Dienstleister)	E-Mail:	XXX.XXXX@XXX.de
Postanschrift:	DSB Straße XXXXX DSB ORT Bayern Deutschland		

IT-Verantwortliche(r)

Als IT-Verantwortliche(r) von "Name des GdW-Unternehmens" ist IT VORNAME IT NAME benannt.

Name:	IT NAME	Telefon:	XXX / XXX XXXXX
Vorname:	IT VORNAME	Mobil:	XXXX / XXXXXXXXX
Position:	IT-LEITER	Telefax:	XXX /XXXXXXXX
Abteilung:	IT-Administration	E-Mail:	IT@Musterunternehmen.de
Postanschrift:	Musterstraße xxxxx Musterstadt Deutschland		

1.1 Verarbeitungen

1.1.1 Verwaltung

1.1.1.1 Wohnungsvergabe / Interessentenverwaltung v. 1.0

Interner Titel: Mietverwaltung / Vermietung

Vergabe von Wohnungen des Unternehmens an Interessenten und somit auch die Verwaltung der Interessentendaten.
Es besteht eine geringfügige Unterscheidung im Verfahren zwischen preisfreiem und preisgebundenem Wohnraum.

Des Weiteren wird als Formular ein Selbstauskunftsbogen als standardisiertes Formular in Papierform/Digital auf der Homepage verwendet.

Die Ablage der erhobenen personenbezogenen Daten erfolgt in Papierform mit Hilfe eines strukturierten Ordnersystems (chronologisch, alphabetisch, je VE, etc.)
Die Speicherung der erhobenen personenbezogenen Daten erfolgt IT-gestützt mit Hilfe des wohnungswirtschaftlichen ERP-Systems (z. B. WODIS; GES, wowinex, immotion, SAP, etc.) sowie mit Hilfe von unternehmenseigenen Excel-Tabellen.

Frei werdende Wohnungen werden bei der (Name des GdW-Unternehmens) z. B. auf dem Online-Portal eingestellt. Potentielle Nachmieter müssen sich bei Interesse jedoch direkt an die (Name des GdW-Unternehmens) wenden (Telefon, Email, persönlich).

Aufgrund der hohen Nachfrage werden gekündigte Wohnungen bei der (Name des GdW-Unternehmens) nicht auf dem freien Markt angeboten. Vielmehr können sich Interessenten für eine Wohnung beim Wohnungsunternehmen melden und auf eine Vormerkliste eintragen lassen. Hierbei werden Kontaktdaten und die gewünschte Art, Lage, Größe und Ausstattung der Wohnung vermerkt. Die Vormerkung gilt für einen Zeitraum von XX Monaten und muss nach Ablauf dieser Frist bei Bedarf durch den Interessenten verlängert/erneuert werden.

Interessenten, die nach dem Besichtigungstermin an der Anmietung der Wohnung interessiert sind, melden sich bei der (Name des GdW-Unternehmens) und werden in das weitere Vergabeverfahren aufgenommen.

Im weiteren Auswahlprozess werden die Interessenten anhand der Angaben auf den Selbstauskunftsbögen durch die Mitarbeiter der Miethausverwaltung bewertet.

Der (am besten) geeignete Interessent wird durch einen Sachbearbeiter einer Bonitätsabfrage bei der Schufa unterzogen. Auf der Rückseite des Selbstauskunftsbogens ist eine Schufa-Klausel hinterlegt, die der Interessent bereits zu Beginn der Bewerbung um eine Wohnung unterzeichnet.

Sollte die Bonitätsprüfung positiv ausfallen, erhält der Interessent bei Vorliegen der übrigen Voraussetzungen die Zusage für die Wohnung. Sollten negative Einträge vorliegen, erfolgt ggf. eine Absage an den Interessenten.

Die Abfrage der Bonität bei der Schufa erfolgt nach folgenden Grundsätzen:

Inhalt dieser Vereinbarung ist, dass Daten zukünftig bereits dann an Vermieter übermittelt werden können, sofern folgende Anforderungen erfüllt sind:

- Die beauskunfteten Daten sind öffentlichen Schuldner- und Insolvenzverzeichnissen entnommen oder
- es handelt sich um sonstige Daten über negatives Zahlungsverhalten, bei denen

- die dem jeweiligen Eintrag zugrundeliegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und
- die Forderung im Falle einer Forderung aus dem Bereich der Kreditwirtschaft (A-Vertrag) einen Betrag in Höhe von 200 Euro oder im Falle einer Forderung aus dem Bereich Handel und Dienstleistung (nicht A-Vertrag) einen Betrag in Höhe von 100 Euro übersteigt.

Systembeschreibung (vordefiniert):	Verwaltet durch Fachverantwortliche
Klassifizierung:	Hohe Auswirkung
Zusätzliche Klassifizierung:	Personenbezogene Daten

Allgemeines zur Verarbeitung

Die Verarbeitung wird für die folgenden Zwecke eingesetzt:

- Anbahnung rechtsgeschäftsähnliches Schuldverhältnis

Zulässigkeit

Rechtsgrundlage

Die Verarbeitung ist zulässig, weil:

- Datenübermittlung an Auskunfteien (BDSG bis Mai 2018)
  Die Übermittlung der personenbezogenen Daten ist zulässig, da die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist und die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und eine der Alternativen des § 28a Abs. 1 Nr. 1 bis 5 BDSG vorliegt (§ 28a Abs. 1 Nr. 1 - 5 BDSG).
- Besondere Arten von Daten (Mitgliederdaten) (BDSG bis Mai 2018)
  Die Verwendung besonderer Arten von Daten (§ 3 Abs. 9 BDSG) ist zulässig, weil es sich um Daten der Mitglieder der politisch, philosophisch, religiös oder gewerkschaftlich ausgerichteten Organisation handelt und die Verwendung für die Tätigkeit der Organisation erforderlich ist (§ 28 Abs. 9 BDSG)
- Rechtspflicht Art. 6 (1) c) DSGVO
  Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt - diese ist zu ergänzen
- Schuldverhältnis (eigener Geschäftszweck) (BDSG bis Mai 2018)
  Die Verarbeitung ist für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses für eigene Geschäftszwecke mit dem Betroffenen erforderlich (§ 28 Abs. 1 Nr. 1 BDSG)
- Vertragserfüllung Art. 6 (1) b) DSGVO
  Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen

Übermittlung ins Ausland

Eine Übermittlung von Daten in einen Drittstaat ist nicht vorgesehen.

Betroffene Personengruppen

- Interessenten

Erlaubte Empfänger

Die folgenden Unternehmen/Institutionen sind erlaubte Empfänger von Daten, die im Rahmen der Verarbeitung "Wohnungsvergabe / Interessentenverwaltung" verarbeitet werden:

- Empfänger:

  Name: z. B. SCHUFA Holding AG

  Telefon: +49 611 - 9278-0

  Telefax: +49 611 - 9278-109

  E-Mail: kontakt@schufa.de

  Postanschrift: Kormoranweg 5
  65201 Wiesbaden
  Hessen
  Deutschland

  Begründung für erlaubten Empfang von Daten aus dieser Verarbeitung:

  Anbahnung eines rechtsgeschäftsähnlichen Schuldverhältnisses --> Berechtigtes Interesse des Unternehmens

  Zweck der Datenübermittlung:

  Bonitätsabfrage bei Auskunftei

Datentypen und Löschfristen

Die folgenden Datentypen werden in der Verarbeitung "Wohnungsvergabe / Interessentenverwaltung" verarbeitet. Zusätzlich wird angegeben, in welchem Zeitraum dieser Datentyp standardmäßig gelöscht wird und welche Löschungsfrist tatsächlich in dieser Verarbeitung eingehalten wird.

Datentyp	Beschreibung	Standard-löschungs-frist	Löschungs-frist	Verschlüs-selt	Klassifi-zierung	Zusätzliche Klassifi-zierung
• Interessentendaten	Name, Vorname, Adresse, Kontaktdaten, Einkommensverhältnisse, Staatsangehörigkeit Arbeitgeber, mit einziehende Personen	1 Jahr nach Eingang der Wohnungsbewerbung	6 Monate		Hohe Auswirkung	Personenbezogene Daten

Zugriffsberechtigungen

Die folgenden Personen oder Personengruppen haben eine Zugriffsberechtigung für die Verarbeitung "Wohnungsvergabe / Interessentenverwaltung":

Person/Gruppe	Begründung	Erteilt	Erloschen
• Sachbearbeiter Vermietung	Durchführung der Vermietung von Wohnungen	01.10.2017	

Meldepflicht

Für die Verarbeitung "Wohnungsvergabe / Interessentenverwaltung" besteht keine gesetzliche Meldepflicht.

Benachrichtigung der Betroffenen

Für die Verarbeitung "Wohnungsvergabe / Interessentenverwaltung" besteht keine gesetzliche Benachrichtigungspflicht.

Begründung: Der Betroffene hat schon auf andere Weise Kenntnis von der Speicherung

Datenschutz-Folgeabschätzung

Eine Datenschutz-Folgeabschätzung ist bzw. war für die Verarbeitung "Wohnungsvergabe / Interessentenverwaltung" nicht erforderlich.

Systembeschreibung, z. B.

Windows
Outlook
Excel
ggf. Vermietungsportal

Anzahl Benutzer: 10

Datenspeicherung und -standort

Datenspeicherung in/auf: Rechenzentrum

Logischer Standort der Daten: Datenbank

Standort der Daten: Germany / Bayern

Begründung(en):

- Vertragserfüllung

1.1.1.2 Risikobewertung

Risikobewertung Wohnungsvergabe			
Erläuterung Im Rahmen der Anbahnung eines rechtsgeschäftsähnlichen Schuldverhältnisses (Mietvertrag) werden personenbezogenen Daten der Interessenten erhoben, verarbeitet und genutzt. Die Datenverarbeitung erfolgt sowohl mit strukturierten Formularen auf Papier, als auch mit Hilfe des Einsatzes von EDV (Tabellenkalkulation, ERP-System, Web-Portal). Ein Scoring wird im Rahmen der Auswahl der Bewerber nicht vorgenommen. Eine Datenübertragung findet im Rahmen der Verarbeitung an folgende Stellen statt: - Wohnungsamt (für öffentlich geförderte Wohnungen) - ARGE - Schufa AG - IT-Systemhaus (Bereitstellung der Software mit der Daten verarbeitet werden --> Hosting) Entsprechend implementierte technische und organisatorische Maßnahmen werden bei der Risikobewertung berücksichtigt.			
Bereich der Auswirk. / Wahrscheinl. B	Auswirkung 67	Wahrscheinlichkeit 24 %	Ursprüngliche Wahrscheinlichkeit 56 %
TOMs zur Minderung des Risikos • Dokumentation Zutrittskontrollmaßnahmen Technische und organisatorische Maßnahmen / Zutrittskontrolle			

Liegt eine Beschreibung / Dokumentation der gesamten am Standort eingesetzten Zutrittskontrollmaßnahmen vor?

Unter Zutrittskontrolle versteht man alle Maßnahmen, die geeignet sind, Unbefugten das Eindringen in geschützte Bereich zu erschweren. Die Spannweite reicht von einer einfachen Schlüsselvergabe bis zu aufwändigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloss eine Zutrittsregelung darstellt.
Zutrittskontrollen sind nur dann wirksam, wenn es keine ungesicherten Zu- / Ausgänge oder andere Zutrittsmöglichkeiten gibt, z.B. über die Kantine etc.

- Archivraum
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Existiert ein eigener Archivraum?

  Es ist Grundsätzlich zu empfehlen Datenträger sowie Akten (Kundendaten, etc.) in einem Archiv zu lagern dessen Zugang kontrolliert werden kann.
  Es sollte geprüft werden, ob ein Archivraum eingerichtet werden kann.

- Auswertungen nach Sicherheitsverstößen
  Technische und organisatorische Maßnahmen / Eingabekontrolle

  Gibt es Anweisungen oder dokumentierte Vorgehensweisen für über das übliche Maß hinausgehende Auswertungen nach Sicherheitsverstößen?

  In besonderen Fällen (z.B. nach dem Bekanntwerden von Sicherheitsverstößen) kann es erforderlich werden, dass das Anwenderverhalten eines Einzelnen oder einer Gruppe von Mitarbeitern temporär über das übliche Maß hinaus geloggt und ausgewertet wird.
  Hierfür sollten Vorgehensweisen dokumentiert und ggf. mit der Mitarbeitervertretung abgestimmt werden.
  Beispiele für Sicherheitsverstöße sind:
  - Menschliche Fehler (z.B. ein Benutzerfehlverhalten gelten, das zu Datenverlust führt)
  - Nichteinhaltung von Leitlinien, Regelungen und Verfahren
  - Verstöße gegen physische Sicherheitsmaßnahmen
  - unkontrollierte Änderungen an Systemen
  - Zugriffsverletzungen

- Benutzerregistrierung
  Technische und organisatorische Maßnahmen / Zugangskontrolle

  Gibt es für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen?

  Vgl. ISO 27001, Annex A.11.2.1: "Benutzerregistrierung"

- Beachtung von Aufbewahrungsfristen
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

  Ist sichergestellt, dass Dokumente und Datenträger, deren Aufbewahrungsfrist abläuft, nachhaltig vernichtet bzw. gelöscht werden?

  Dokumente und / oder Datenträger sind erst nach Ablauf, aber dann zuverlässig, zu löschen oder zu vernichteten. Wird das nicht konsequent umgesetzt, so können vorgefundene veraltete Daten und Dokumente z.B. bei Betriebsprüfungen oder Ermittlungsverfahren als Beweismittel verwertet werden.

- Datenschutzschulungen
  Technische und organisatorische Maßnahmen / Weitergabekontrolle

Sind die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult worden?

Zuständig für die Schulung der Mitarbeiter auf den Datenschutz ist der Beauftragte für den Datenschutz.

- Ausscheiden Mitarbeiter
  Technische und organisatorische Maßnahmen / Weitergabekontrolle

  Gibt es Regelungen für die Behandlung ausscheidender, insbesondere gekündigter Mitarbeiter?

  In der Regel entbindet ein Ausscheiden aus dem Unternehmen den Arbeitnehmer nicht von der Verpflichtung auf das Datengeheimnis. Entsprechende Passagen können sich im Arbeitsvertrag oder in der Kündigung (wenn vom Arbeitgeber gekündigt wird) finden.

- Datenverschlüsselung
  Technische und organisatorische Maßnahmen / Weitergabekontrolle

  Erfolgt die Übermittlung der weitergegebenen Daten verschlüsselt?

  Bei der Datenweitergabe ist die erforderliche Sorgfalt anzuwenden:
  Da nicht verschlüsselte Mails im Internet wie eine Postkarte ausgelesen werden können, sollte die Übermittlung per E-Mail nur verschlüsselt erfolgen.
  Entsprechend sind Dateitransfers über das Internet nur über verschlüsselte Verbindungen abzuwickeln.

- Brennbare Gegenstände im DV-Bereich
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Befinden sich im DV-Bereich keine brennbaren Gegenstände wie Reinigungsmittel, Papiervorräte/-abfälle (außer Tagesbedarf/Tagesanfall) oder Vorhänge?

  Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. Z. B. sollte das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager untergebracht sein.

- Existenz maschineller Zutrittskontrollsysteme
  Technische und organisatorische Maßnahmen / Zutrittskontrolle

  Existieren maschinelle Zutrittskontrollsysteme?

  Gibt es am Standort maschinelle Zutrittskontrollsysteme zur Überwachung des Betretens und evtl. auch Verlassens eines Gebäudes / eines Gebäudeteils?
  Werden eventuell biometrische Kontrollsysteme (Handflächen, Iris-Scanner, Fingerabdruck-Leser) eingesetzt, die durch die Überprüfung eines Personenmerkmals eine höhere Sicherheitsstufe darstellen?

- Einsatz von Verschlüsselung auf Datei- / Verzeichnisebene
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

  Wird von der Verschlüsselung der Daten auf Dateiebene / Verzeichnisebene Gebrauch gemacht?

  Durch Verschlüsselung einzelner Dateien oder kompletter Verzeichnisse können Informationen vor unautorisiertem Zugriff geschützt werden.

- Einsatz von Verschlüsselung für mobile Datenträger
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

Werden die Informationen auf mobilen Datenträgern ausreichend davor geschützt, im Verlustfall ausgelesen werden zu können?

Durch den Einsatz von Festplattenverschlüsselung können die Informationen auf Laptops vor unbefugtem Zugriff geschützt werden.
Die modernen Lösungen decken meistens USB-Datenträger mit ab.
Festplattenverschlüsselung sollte bei Laptops als Standardmaßnahme eingesetzt werden.
Wenn USB-Datenträger nicht verschlüsselt werden, so sollten diese entweder ganz verboten werden oder zumindest eine organisatorische Regelung für den Einsatz davon verfasst werden.

- Einsatz sicherer Verschlüsselungsalgorithmen
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

  Wird die Software eines anerkannten Herstellers eingesetzt, so dass von hinreichend sicheren Verschlüsselungsalgorithmen ausgegangen werden kann?

  Bei den anerkannten Herstellern von Verschlüsselungs- und Signatursoftware ist davon auszugehen, dass hinreichend sichere Verschlüsselungsalgorithmen eingesetzt werden.
  Auf den Webseiten des BSI kann verglichen werden, ob der eingesetzte Mechanismus noch als ausreichend sicher gilt.
  Wenn der Hersteller keine Angaben zum eingesetzten Verschlüsselungsalgorithmus machen will oder kann, so ist vom Einsatz abzusehen.

- Entsorgung von Papierdokumenten und Datenträgern
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

  Gibt es eine Anweisung darüber, wie mit nicht mehr benötigten Datenträgern umzugehen ist (dazu gehört auch beschriebenes oder bedrucktes Papier)?

  Vgl. ISO 27001, Annex A.10.7.2 „Entsorgung von Medien“:
  Entsprechende verschließbare Tonnen sollten für Papierdokumente und Datenträger vorhanden sein und regelmäßig geleert werden. Die Mitarbeiter sind über die Notwendigkeit der ordnungsgemäßen Entsorgung und das Vorgehen zu informieren.

- Erläuterung
  Technische und organisatorische Maßnahmen / Weitergabekontrolle

  Wurden allen Beteiligten die Belange der Datensicherheit und des Datenschutzes erläutert?

- Dokumentation der bei der Übermittlung eingesetzten Programme
  Technische und organisatorische Maßnahmen / Weitergabekontrolle

  Erfolgt eine Dokumentation der für die selbsttätige Übermittlung einzusetzender Programme?

  Ist intern dokumentiert, mit welchen Tools oder Programmen die selbsttätige Datenübermittlung erfolgt? (z. B. an den Rentenversicherungsträger)

- Dokumentation des Auswahlverfahrens
  Technische und organisatorische Maßnahmen / Auftragskontrolle

  Hat die verantwortliche Stelle die Entscheidung für die Wahl eines bestimmten Auftragnehmers dokumentiert?

  Die Dokumentation dient als Beleg für die gesetzlich geforderte Auswahl des Auftragnehmers unter Datenschutzgesichtspunkten.

- Dokumentation des Auswahlverfahrens
  Technische und organisatorische Maßnahmen / Auftragskontrolle

Hat die verantwortliche Stelle die Entscheidung für die Wahl eines bestimmten Auftragnehmers dokumentiert?

Die Dokumentation dient als Beleg für die gesetzlich geforderte Auswahl des Auftragnehmers unter Datenschutzgesichtspunkten.

- Existenz aktuelles Notfallhandbuch
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Existiert ein Notfallhandbuch und wird dieses laufend aktualisiert?

  In einem Notfallhandbuch sind alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen dokumentiert. Das Notfallhandbuch ist so verfasst, dass ein sachverständiger Dritter in der Lage ist, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen.

- Einlagerung und Ausgabe von Datenträgern bzw. Dokumenten
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Erfolgt im Archiv die Ein- und Ausgabe von Datenträgern nur durch die autorisierten Mitglieder der Archivverwaltung?

  Die Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.
  In der Archivordnung ist die Datenverwaltung zu regeln. Die Ein- und Ausgabe vom Archiv ist zu dokumentieren.

- Einhaltung von Sicherheitsregelungen
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wird regelmäßig überprüft, ob die Mitarbeiter die Sicherheitsvorschriften einhalten? Wurden Maßnahmen zur Sicherstellung der Einhaltung der Vorschriften eingeleitet?

- Regelwerk zur Zugangskontrolle
  Technische und organisatorische Maßnahmen / Zugangskontrolle

  Liegt eine Beschreibung der Zugangskontrollmaßnahmen vor?

  Die Beschreibung sollte auf die Anforderungen der verantwortlichen Stelle eingehen und auf Grund dieser Anforderungen klar die Zugangs-Regeln für Nutzer oder Benutzergruppen des EDV-Systems festlegen.
  Vgl. ISO 27001, Annex A.11.1.1: "Regelwerk zur Zugangskontrolle"

- Sicherheitssoftware Fremdhersteller
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

  Wird für die Gewährleistung der Datensicherheit und der Zugriffssicherung eine spezielle Sicherheitssoftware eines Fremdherstellers eingesetzt?

  Hierunter fallen sogenannte „Intrusion Detection“ Systeme, „Leakage Prevention“ Systeme und Verschlüsselungsanwendungen.

- Sichere Entsorgung oder Weiterverwendung von mit Speichermedien ausgestatten Geräten
  Technische und organisatorische Maßnahmen / Zugriffskontrolle

Gibt es eine Anweisung darüber, wie bei der Entsorgung oder Weiterverwendung von Geräten vorzugehen ist, die mit Speichermedien ausgerüstet sind?

Auch Multifunktionsgeräte wie Scanner-, Fax- und Druckereinheiten können über eingebaute Speichermedien verfügen, auf denen sich noch Dokumente befinden. Vor der Entsorgung oder Weiterverwendung ist sicherzustellen, dass hierdurch keine personenbezogenen Daten an unberechtigte Dritte weitergegeben werden.
Vgl. ISO 27001, Annex A.9.2.6 „Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln"

- Verpflichtung
  Technische und organisatorische Maßnahmen / Weitergabekontrolle

  Wurden alle Personen, die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, zur Einhaltung auf das Datengeheimnis verpflichtet?

  Existieren von allen Mitarbeitern, die mit der Verarbeitung von personenbezogenen Daten befasst sind, Verpflichtungserklärung gemäß § 5 Bundesdatenschutzgesetz (BDSG) zur Wahrung des Datengeheimnisses?
  Ist ein Verfahren etabliert, wie vorzugehen ist, wenn sich ein Beschäftigter weigert, die Verpflichtungserklärung zu unterzeichnen?
  Vgl. ISO 27001, Annex A.6.1.5 „Vertraulichkeitsvereinbarungen"

- Vertragliche Verpflichtung Auftragsdatenverarbeiter
  Technische und organisatorische Maßnahmen / Auftragskontrolle

  Sind alle Auftragsdatenverarbeiter (z.B. der Steuerberater oder ggf. der Betreiber eines externen Archivs) vollständig vertraglich verpflichtet?

  Entnommen aus der Begründung für eine Verschärfung der in § 43 2b BDSG geregelte Kontrolle der Auftragsdatenverarbeiter im Rahmen der BDSG-Novelle:
  „Nach Nummer 2b handelt der Auftraggeber ordnungswidrig, wenn er entgegen § 11 Absatz 2 Satz 2 den Auftrag nicht schriftlich erteilt oder nicht die vorgegebenen Festlegungen hinsichtlich der Datenerhebung oder -verwendung sowie die technischen und organisatorischen Maßnahmen und Unterauftragsverhältnisse festlegt. Die Aufsichtspraxis weist darauf hin, dass ein vollständiger schriftlicher Auftrag die Ausnahme ist."

- Regelungskatalog erfüllt?
  Technische und organisatorische Maßnahmen / Auftragskontrolle

  Erfüllt der schriftliche Auftrag die Anforderungen des Regelungskatalogs des § 11 Abs. 2 BDSG? (Alternativ Art. 28 ff DSGVO)

  § 11 Abs. 2 BGDS enthält einen Katalog von zehn Punkten, welche in dem Vertrag enthalten sein müssen. Sie betreffen:
  1. Gegenstand und Dauer des Auftrags
  2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung, Art der Daten und Kreis der Betroffenen
  3. die zu treffenden technischen und organisatorischen Maßnahmen
  4. Berichtigung, Sperrung und Löschung von Daten
  5. die nach § 11 Abs. 4 BDSG bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen
  6. etwaige Berechtigungen zur Begründung von Unterauftragsverhältnissen
  7. Kontrollrechte des Auftraggebers und Duldungspflichten des Auftragnehmers
  8. mitzuteilende Verstöße bei dem Auftragnehmer
  9. Umfang der Weisungsbefugnis

10. Rückgabe überlassener Datenträger und Löschung gespeicherter Daten nach Auftragsende.

- Vorherige Information über den Auftragnehmer
  Technische und organisatorische Maßnahmen / Auftragskontrolle

  Lagen dem Auftraggeber vor der Erteilung des Auftrages Informationen über den zukünftigen Auftragnehmer vor?

  Hat eine Leistungsbeschreibung vorgelegen, welche auch die technischen und organisatorischen Maßnahmen umfasst hat?
  Haben datenschutzrechtliche Aspekte bei der Auswahl des Auftragnehmers eine Rolle gespielt?
  Konnte der Auftragnehmer einen Ansprechpartner für den Datenschutz / einen Datenschutzbeauftragten konkret benennen?

- Vorherige Information über den Auftragnehmer
  Technische und organisatorische Maßnahmen / Auftragskontrolle

  Lagen dem Auftraggeber vor der Erteilung des Auftrages Informationen über den zukünftigen Auftragnehmer vor?

  Hat eine Leistungsbeschreibung vorgelegen, welche auch die technischen und organisatorischen Maßnahmen umfasst hat?
  Haben datenschutzrechtliche Aspekte bei der Auswahl des Auftragnehmers eine Rolle gespielt?
  Konnte der Auftragnehmer einen Ansprechpartner für den Datenschutz / einen Datenschutzbeauftragten konkret benennen?

- Schriftliche Weisungen
  Technische und organisatorische Maßnahmen / Auftragskontrolle

  Erfolgen Weisungen schriftlich?

  Schriftliche Weisungen verhindern Missverständnisse und dienen beiden Seiten als Nachweis in Zweifelsfällen. Folgende Verfahren sind denkbar:
  Sollten auch mündliche Weisungen - etwa in Eilfällen erforderlich - sein, sollten diese schriftlich bestätigt werden.

- Fenster im DV-Bereich
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Sind die Fenster so ausgeführt, dass hinsichtlich DV-Bereich von einem Sicherheitsbereich gesprochen werden kann?

  Folgende Bedingungen müssen dazu erfüllt sein:
  - Die Fenster müssen gegen unbefugtes Öffnen gesichert sein, z.B. durch in die Fenstergriffe integrierte Schlösser (Besonders wichtig bei klimatisierten Räumen)
  - Das Material muss aus Panzerglas oder zumindest einbruchshemmender Verglasung bestehen.
  - Falls die Fenster von außen leicht erreichbar sind, so müssen sie in die Außenhautsicherung mit einbezogen werden (d.h., es sind Glasbruch- und Öffnungsmelder zu installieren)
  - Falls die Fenster von außen leicht einsehbar sind, so ist ein Sichtschutz zu installieren (z.B. durch aufgeklebte sog. Milchglasfolien)

- Qualität der Räumlichkeiten für Netzwerk-Ausstattung
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

Genügen die Räume, in denen Netzwerk-Ausstattung untergebracht ist, noch den aktuellen Ansprüchen?

Generell müssen die Räumlichkeiten, in denen sich Netzwerkequipment befindet, abschließbar sein, ferner möglichst klimatisiert und fensterlos.
Wenn eine Organisation für mehrere Jahre an einem Standort bleibt, so kommt es häufig vor, dass die Räume mit Netzwerk-Equipment „zugestellt" werden und/oder dass sie durch ungeeignete Provisoriumsräume ergänzt werden.

- USV
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Ist dokumentiert, welche Geräte bei einem Ausfall der Stromversorgung wie lange versorgt werden?

  Aus diesem Datum ergibt sich die benötigte Leistung und damit auch die Größe der USV Installation, welche von einem kleinen 19´´ Einbaugerät bis zu einer raumfüllenden Akkumulator-Installation reichen kann.
  In kleinen Rechenzentren oder in kleinen Gewerken, die nur eine kleine Anzahl von Serverschränken besitzen, wird die USV Anlage üblicherweise nicht in einem gesonderten Raum, sondern im Rechnerraum direkt im oder neben dem Schrank installiert.

- Klimaanlage
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Die Raumtemperatur im Serverraum muss auf ein angemessenes Maß geregelt sein.
  Hierfür ist der Einsatz einer Klimaanlage erforderlich

- Feuerlöscher und Flutungsanlagen
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Sind ausreichend geeignete Feuerlöscher/Flutungsanlagen sowie das richtige Löschmittel im Einsatz und wird dabei auf Einheitlichkeit geachtet (z.B. ausschließlich CO2 Löscher)?

  Die Sofortbekämpfung aufkommender Brände ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Serverraum, Raum mit technischer Infrastruktur oder Belegarchiv anzustreben.
  Für elektronische Geräte sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird durch Verdrängung des Sauerstoffs erreicht, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten
  Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.
  Wasserlöscher mit Eignung für Brandklasse A bis 1000 V sind durchaus für elektrisch betriebene Geräte geeignet.
  Für elektronisch gesteuerte Geräte, z. B. Rechner, sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird durch Verdrängung des Sauerstoffs erreicht, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten.
  Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind.

- Wartung Brandschutzgeräte
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

Findet eine regelmäßige Wartung und Überprüfung der Rauchmelder und Handfeuerlöscher statt?

- Untersuchung Katastrophenmöglichkeiten
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wurden alle in Frage kommenden Katastrophenmöglichkeiten untersucht (Streik, Personalausfall, Sachbeschädigung, Feuer, Explosion, Erdbeben, Wassereinbruch, längere Störungen oder Ausfälle der Infrastruktur)?

  Wurden dabei besondere Risikofaktoren der Gebäudelage berücksichtigt, wie z.B.
  - Lage des Gebäudes in einer Einflugschneise militärischer oder ziviler Flughäfen
  - Lage des Gebäudes in unmittelbarer Nachbarschaft zu Brennstofflagern wie z.B. Raffinerien, Tankstellen, Benzin- oder Heizöllager?
  - Lage des Gebäudes an einem demonstrationsgefährdeten Ort?

  Eine ausführliche Aufstellung und Erläuterung möglicher Katastrophenfälle findet sich auch im Grundschutzhandbuch des BSI - Bundesamt für Sicherheit in der Informationstechnik. Es ist über die Webseite (www.bsi.de) öffentlich zugänglich.

- Publikation Notfallkonzept
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wurde das Notfallkonzept den betroffenen Beteiligten (Krisenstab, Betroffene) rechtzeitig bekannt gemacht?

  Das Notfallkonzept sollte bereits unmittelbar nach seiner Erstellung und nicht erst im Katastrophenfall zuständigen Stellen ausgehändigt werden. Soweit möglich, sollten Betroffene und zuständige Stellen in die Erstellung des Notfallkonzeptes eingebunden werden.

- Schutz vor Diebstahl oder Zerstörung
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Sind Die Backups ausreichend vor Diebstahl und Zerstörung geschützt?

  Sicherungskopien dürfen nie im gleichen Gebäude oder Brandabschnitt wie das DV-System aufbewahrt werden. Die Datensicherung muss entweder direkt auf einem Server an einem anderen Standort erstellt werden, oder Datenträger mit Datensicherungen sind entsprechend an einem ausgelagerten Ort aufzubewahren.

- Verantwortlichkeiten
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wurden die für die Sicherung verantwortlichen Personen namentlich benannt und wurde dieses dokumentiert?

  Es muss namentlich und schriftlich festgehalten werden wer für welche Datensicherung verantwortlich ist. Operatoren müssen festgelegt werden.

- Kapazitätsplanung
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wurde eine Kapazitätsplanung durchgeführt?

  Eine Kapazitätsplanung und Zuwachsschätzung für den Zeitraum von 2 Jahren muss erfolgen.

- Funktionalitätstest
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wird regelmäßig getestet, ob das Backup brauchbar ist?

Es ist regelmäßig zu testen, ob sich aus dem Backup funktionsfähige Datensätze oder Systeme wiederherstellen lassen. Diese Tests sollen nicht auf dem Produktivsystem, sondern in der Testumgebung stattfinden.

- Löschungsfristen
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Ist sichergestellt, dass Daten, deren Löschungsfrist abläuft, nachhaltig gelöscht bzw. vernichtet werden?

  Das Archiv muss so organisiert sein, dass Dokumente oder Datenträger erst nach Ablauf aber dann zuverlässig gelöscht oder vernichtet werden.
  siehe Archivordnung und gesetzlichen Vorgaben zu den verschiedenen Löschungsfristen.
  Diese Fristen sind zu dokumentieren und umzusetzen.

- Kompetenzregelungen IT- und Fachabteilungen
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Wurden die Kompetenzen und Verantwortungsbereiche zwischen der IT-Abteilung und anderen Fachabteilungen eindeutig geregelt?

  Gibt es Stellenbeschreibungen oder Organisationsstrukturen, aus denen die Verantwortungsbereiche hervorgehen?

- Private Nutzung von unternehmenseigenen Laptops
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Ist die private Nutzung von firmeneigenen Laptops explizit verboten?

  Wenn Mitarbeiter die firmeneigenen Computer privat nutzen dürfen, ist die Wahrscheinlichkeit hoch, dass illegales Material darauf abgespeichert wird oder dass Schadsoftware darauf gelangt, welche mit dem Anschluss des Geräts an das firmeneigene LAN weitere Computer infiziert.
  Hinzu kommen mögliche Lizenz-Probleme durch das Nicht-Untersagen der privaten Nutzung.
  Die private Nutzung von firmeneigenen Computern ist baldmöglichst zu untersagen.

- Zutrittsschutz im DV-Bereich
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Sind die Maßnahmen zum Zutrittsschutz so ausgeführt, dass hinsichtlich DV-Bereich von einem Sicherheitsbereich gesprochen werden kann?

  Folgende Bedingungen müssen dazu erfüllt sein:
  - Die Anzahl der nach außen führenden Türen ist auf das unbedingt nötige Minimum zu beschränken.
  - Die Türen sind ständig geschlossen zu halten und sich von außen nur mit einer Codekarte oder einem Schlüssel öffnen lassen.
  - Für den DV-Bereich sollte ein eigener Schließbereich mit besonderen Sicherheitsschlüsseln existieren.
  - Fluchttüren dürfen sich nur von innen öffnen lassen.

- Wiederanlaufplanung DV-Bereich im Katastrophenfall
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

  Gibt es für den DV-Wiederanlauf eine schriftliche Unterlage (Zusammensetzung und Aufgaben des Katastrophenstabes)?

- Zutritt zum Archiv
  Technische und organisatorische Maßnahmen / Verfügbarkeitskontrolle

Ist der Zutritt zum Archiv auf einen genau festgelegten Personenkreis eingeschränkt? Eine Zutrittskontrolle kann z.B. durch eine entsprechende Schlüsselverwaltung/Schlüsselausgabe erfolgen. Voraussetzung ist, dass das Archiv verschlossen werden kann und muss.